Robert S. Smith (pro hac vice)
Law Offices Robert S. Smith
57 Pratt Street, Suite 513
Hartford, CT 06103
Voice: 860-983-5838
Email: smith@i-p-counsel.com
www.i-p-counsel.com

Attorney for Defendant Doe No. 30



UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF TEXAS

HOUSTON DIVISION

| | |
|---|---|
| SIEMANS PRODUCT LIFECYCLE MANAGEMENT SOFTWARE INC., Plaintiffs, v. DOES 1-100, Defendants. | CIVIL ACTION NO. 4:16-CV-1422 (KPE) |

**MOTION TO QUASH SUBPOENA**

Defendant Doe No. 30 hereby respectfully requests that this Court (1) quash a subpoena purportedly served upon Comcast on or about 5/25/2016 to produce his/her name, address, telephone number, email address and any other information that would aid Plaintiff in determining the identity of the account holder or in the alternative (2) declare that no valid subpoena has properly been served upon the Comcast pursuant to Fed. R. Civ. P. 45.

As grounds therefor, Movants state as follows:

1. The purported subpoenas would require that Comcast disclose to plaintiffs a list of persons who have downloaded certain content, despite these persons' privacy interest in avoiding such disclosure and despite their legitimate expectation of privacy in anonymously accessing and/or downloading information of interest to them from the Internet. In addition to being unduly burdensome and unfair to movants, this request raises concerns of tremendous constitutional significance, that should not be resolved lightly or without careful analysis of their implications.

2. One complicating factor is that, with respect to the purported log of IP addresses provided by Plaintiff, people who briefly joined the torrent swarm and may never have uploaded any material part of the file/video cannot be distinguished from people who downloaded the complete file, then observed the copyright notice thereon and then consciously allowed the torrent to seed and thus upload/distribute the software to others. Accordingly, compliance with the subpoenas would result in the disclosure of the identities of people who did not download any or any material part of the copyrighted video, and who plaintiff has no right or need to learn identifying information. These considerations are in addition to concerns about the manner of collection to plaintiff's log as well as the validity thereof.

3. The Supreme Court has repeatedly reaffirmed the constitutional right to speak anonymously, see, e.g., MacIntyre v. Ohio Elections Commission, 514 U.S. 334, 342 (1995), and at least one court has recognized the importance of protecting anonymous speech in the Internet context. See ACLU v. Miller, 977 F. Supp. 1228, 1231 (N.D. Ga. 1997).

4. This Court need not reach these constitutional issues, however, because are in support of a case that is not properly before this Court. The pending case lacks personal jurisdiction. The Court lacks personal jurisdiction over the defendants named in the Complaint, and the underlying case must therefore be dismissed for that reason. Doe No. 30 that is alleged to have infringed does not reside or work in this judicial

district or any place within at least 300 miles of any part of Texas. Furthermore Doe No. has never been in Texas and has never even been within 300 miles of any part of Teas. As will be discussed further herein, merely being in a torrent swarm at any instant of time can occur without making any distribution of any part of any file. It follows with still greater force that merely being in a torrent swarm at any instant of time can occur without making any distribution of any part of any file in Texas. Furthermore, the purported download was Product lifecycle management (PLM) software that the plaintiff characterizes on a web site as an information management system that can integrate data, processes, business systems and, ultimately, people in an extended enterprise. PLM software allows you to manage this information throughout the entire lifecycle of a product efficiently and cost-effectively, from ideation, design and manufacture, through service and disposal and asserts that:

Diverse functions and technologies converge through PLM, including:

- Product data management (PDM)
- Computer-aided design (CAD)
- Computer-aided manufacturing (CAM)
- 3D computer-aided engineering (CAE) and simulation
- Predictive engineering analytics
- Mechatronic system simulation (1D CAE)
- Finite element analysis (FEA)
- Modal testing and analysis
- Digital manufacturing
- Manufacturing operations management (MOM)

Doe No. 30 has no conception of the nature, purpose or utilization of such software.

5. The anonymity of persons accessing Internet web sites should not be breached in aid of a case not properly filed in this Court. Indeed, in a similar situation, Columbia Insurance Co. v. SEESCANDY, Inc., 185 F.R.D. 573, 578-80 (N.D. Cal 1999), the court held that it would not breach the anonymity of an Internet poster without first requiring plaintiff to show the adequacy of the Complaint. See id. ("[P]laintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss. A conclusory pleading will never be sufficient to establish this element.")

6. The subpoenas should be quashed for the reason (in addition to those set forth above) that the complaint alleges a specific Internet protocol address was connected to

a torrent swarm at one instant in time. It does not allege how long the particular Internet program protocol address was connected to the swarm. All file transfers require a finite amount of time to occur. The defendant does not concede that the IP address represents a connection from his computer. However, even if his computer was connected to the swarm at any given instant, without even an allegation of an extended connection time, much less documentation thereof, it is impossible to establish that any data was uploaded by his computer. Thus it is impossible to substantiate the allegation (1) of distribution any copyrighted material, (2) much less a material part of any copyrighted material, (3) much less a material part of any copyrighted material in Texas.

7. A specific IP number may be identified in the swarm without the download or upload any material part of any given video/file. For example, a computer operator may (1) turn off his computer and never complete the download; (2) decide the download is too slow and terminate the process; or (3) decide for some other reason to abort the process. Thus, even if a particular computer is operated by the person associated with IP number there is still the possibility that no material part of a file/video ever being in the possession of the person associated with that IP number. A download of a small part of a file will inherently be a fair use under the copyright laws, just as the copying of a paragraph from a copyrighted book is a fair use.

8. The complaint alleges in paragraph 3: "However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user *who has already downloaded the file* that together comprises the whole." The statement is materially misleading because the reality is that each new file downloader might receive one or more pieces of the data that comprises the whole from others in the swarm who have already downloaded the particular pieces of the entire data that comprises the whole. The individual pieces are not marked with copyright notices and it is not possible to ascertain the nature of the downloaded material until all of the pieces have been downloaded. The individual pieces are typically between 32 kB and 16 MB. Pieces are typically downloaded non-sequentially and are rearranged into the correct order by the BitTorrent Client. http://en.wikipedia.org/wiki/BitTorrent The difference is not academic because a computer user can upload pieces of the file before even having

all of the pieces which would enable either computer user to determine if the file/video is protected by copyright.

9. The filename will not tell a computer user if any given file is protected under copyright laws. Thus, the user cannot even determine if the file should not be accessed at any time prior to complete download of the entire file. A prudent user should not be prevented from downloading every file because it might be found to be copyrighted after download. Such a result would constitute a substantial prior restraint on the rights of the individual members of the public. The computer user will never have any notice of copyright prior to downloading the entire file or video. Thus, the computer use is clearly not committing deliberate infringement particularly if the computer user never completes the download, never opens the file or the computer crashed before the entire file is downloaded. If the computer user does not open the file or does not carefully review the small parts thereof asserting rights under the copyright law, he or she will not have any notice of such rights.

10. The. complaint and Subpoena in this matter is still another suit in which a copyright infringement plaintiff seeks to "tag" a defendant based solely on an IP address. However, an IP address is not equivalent to a person or entity. It is not a fingerprint or DNA evidence – indeed, far from it. In a remarkably similar case in which an adult entertainment content producer also sought expedited discovery to learn the identity of persons associated with IP addresses, United States District Judge Harold Baker of the Central District of Illinois denied a motion for expedited discovery and reconsideration, holding that, "IP subscribers are not necessarily copyright infringers...The infringer might be the subscriber, someone in the subscriber's household, a visitor with her laptop, a neighbor, or someone parked on the street at any given moment." Order of Apr. 29, 2011, VPR Internationale v. DOES 1-1017, No. 2:11-cv-02068 (Central District of Illinois) (Judge Harold A. Baker) [hereinafter VPR Internationale Order]. The point so aptly made by Judge Baker is that there may or may not be a correlation between the individual subscriber, the IP address, and the infringing activity. Id. The risk of false identification by ISPs based on internet protocol addresses is vividly illustrated by Judge Baker when he describes a raid by federal agents on a

home allegedly linked to downloaded child pornography. The identity and location of the subscriber were provided by the ISP (in the same fashion as Plaintiff seeks to extract such information from Wide Open West.) After the raid revealed no pornography on the family computers, federal agents eventually learned they raided the wrong home. The downloads of pornographic material were traced to a neighbor who had used multiple IP subscribers' Wi-Fi connections. Id. This risk of false identification and false accusations through disclosure of identities of internet subscribers is also presented here. Given the nature of the allegations and the material in question, should this Court force Comcast to turn over the requested information, DOE No. 30 would suffer a reputational injury.

11. If the mere act of having an internet address can link a subscriber to copyright infringement suits, internet subscribers such as DOE No. 30 will face untold reputational injury, harassment, and embarrassment. The reputational risk that Judge Baker found to be an undue burden is equally presented here: "[W]hether you're guilty or not, you look like a suspect." Id. at 3. Moreover, this case presents the same extortion risk that so concerned Judge Baker:

> "Could expedited discovery be used to wrest quick settlements, even from people who have done nothing wrong? The embarrassment of public exposure might be too great, the legal system too daunting and expensive, for some to ask whether Celestial, Inc. has competent evidence to prove its case."
>
> "In its order denying the motion for expedited discovery, the court noted that until at least one person is served, the court lacks personal jurisdiction over anyone. The court has no jurisdiction over any of the Does at this time; the imprimatur of this court will not be used to advance a "fishing expedition by means of a perversion of the purpose and intent" of class actions. Order, d/e 9."

12. Plaintiffs in these types of cases use discovery to extort settlements from anonymous defendants who wish to avoid the embarrassment of being publicly associated with this type of allegation. Such abuse of the discovery process cannot be allowed to continue.

13. Additionally, this subpoena should not have been issued in the first place because the information sought is not relevant to Plaintiff's allegations. Implicit in the rule granting subpoena power is a requirement that the subpoena seeks relevant information. See Syposs v. United States, 181 F.R.D. 224, 226 (W.D.N.Y. 1998)("the reach of a subpoena issued pursuant to [FED. R. CIV. P. 45] is subject to the general relevancy standard applicable to discovery under [FED. R. CIV. P. 26(b)(1)]."). The information linked to an IP address cannot give you the identity of the infringer. VPR Internationale Order, at 2. Because the infringer could have been anybody with a laptop passing within range of the router, the information sought by Plaintiff is not relevant to the allegations in any way. Id. Moreover, even if the information has some small amount of relevance to the claim—which it does not—discovery requests cannot be granted if the quantum of relevance is outweighed by the quantum of burden to the defendant. FED. R. CIV. P. 26(b)(2)(C)(iii). Plaintiff's request fails that balancing test. Given that DOE No. 30 was only one of many persons who could have used the IP address in question, the quantum of relevance is miniscule at best. However, as discussed above, the burden to DOE No. 30 is severe. The lack of relevance on the one hand, measured against the severe burden of risking a significant reputational injury on the other, means that this subpoena fails the Rule 26 balancing test. Id. Plaintiff's request for information is an unjustified fishing expedition that will cause reputational injury, prejudice, and undue burden to DOE No. 30 if allowed to proceed. Good cause exists to quash the subpoena served on Comcast to compel the disclosure of the name, address, telephone numbers and e-mail addresses of DOE No. 30.

14. Thus, the major issues may be summarized as:

a. burdensome and unfair to movants

b. brief connections to a torrent swarm may not result download and or upload of a material part of any file

c. lack of jurisdiction over the defendant

d. impossibility of computer user knowing if a file is Copyrighted

e. ambiguity of person associated with any IP number

f. disclosure facilitates extortion from persons who have done nothing wrong

g. no service has been made on any defendant, thus, the court lacks personal jurisdiction over anyone

15. For each of the above reasons, the subpoenas are invalid. Moreover, the Movants are not subject to personal jurisdiction in this Court. Nonetheless, out of an abundance of caution, Movants are filing the within motion rather than simply ignoring the invalid subpoenas as Rule 45 would permit them to do. This motion is not intended to constitute a general appearance, and does not waive or acknowledge personal jurisdiction over any Movant by this Court, said personal jurisdiction being expressly denied.

Accordingly, it is requested that the Defendant's motion be granted.

The Defendant
DOE No. 30

**/Robert S. Smith/**

ROBERT S. SMITH

LAW OFFICES OF ROBERT S. SMITH
Attorney for Defendant
Federal Bar Number ct10975
57 Pratt Street, Suite 513
Hartford, CT 06103
VOICE (860) 983-5838
EMAIL smith@i-p-counsel.com